Busnes | Business Cymru | Wales

Llywodraeth Cymru Welsh Government

GUIDANCE, DOCUMENT

Business Crime: Business Scams

fraud and scams have been both aided and hindered by advances in technologies. It’s given fraudsters and scammers more avenues to exploit and extort, but also made the fight against fraud a little easier.

First published: 7 May 2024

Last updated: 7 May 2024

In this page

Introduction

Fraud and scams have been in existence as long as people have been on this planet. The history of fraud dates back to 300 B.C. when a Greek merchant took out a large insurance policy against a boat of cargo that was due to be delivered. He planned to sink an empty boat, keep the loan and then sell the corn. But, like many ill-thought out scams since, it didn't work out.

Nowadays, fraud and scams have been both aided and hindered by advances in technologies. It's given fraudsters and scammers more avenues to exploit and extort, but also made the fight against fraud a little easier.

The term 'fraud' is broad in definition but, in its simplest terms, it can be defined as using trickery or deception to gain a dishonest advantage over another business, individual or organisation.

Across the different types of fraud, one simple fact remains. Fraud has a huge cost to individuals, organisations and the wider economy. According to the National Fraud Authority's 2013 Annual Fraud Indicator, the UK economy lost £52bn to fraud in 2013.

For businesses, the impact of fraud can be far-reaching. Fraud against small and medium-sized enterprises (SMEs) can have a detrimental impact and many struggle to recover from the financial damage to the business. If a business does survive the financial cost, its reputation might be damaged because they are perceived as an unsafe organisation with which to do business. Businesses, both large and small, may also see increases in the cost of doing business due to increased security measures.

In Wales, a significant amount of resource goes into combatting the effects of fraud and scams, and raising awareness among businesses and consumers. In 2010, the Welsh Fraud Forum met for the first time, giving Welsh SMEs the chance to hear

from some of the UK’s leading experts in fraud prevention and detection.

The forum now meets every year and further work is underway to raise awareness of the effects of fraud in Wales. Fraudsters and scammers don’t discriminate against who they attack. Whether a victim is rich or poor, a small business or a large business, anyone can fall victim.

This is the first edition of Buisness Scams, aimed at outlining key crimes that can affect consumers and businesses. It is designed to be a go-to guide for information and advice on what to look out for and, importantly, where to turn for advice and reporting.

e-Crime

E-Crime can be difficult to detect and punish because of its technical complexity and its ability to adapt with new technology and developments in software protection. New threats emerge with an alarming degree of regularity, with potentially devastating consequences.

So, what is e-Crime?

e-Crime refers to criminal activity where a computer is the source, tool, target, or place of a crime. Despite the inevitable references to ‘computers’ or ‘online activity’, e-crime covers a multitude of ’traditional’ crimes such as fraud and theft.

Simply maintaining a better understanding of the threats and risks a business could face could have a significant impact on the ability to respond to them.

Here are a few common threats to look out for and tips on what action to take if the need occurs:

Malware and Ransomware

Malware; short for **“malicious software”**, are computer programmes designed to infiltrate and damage computers without the user’s consent. Malware covers all of the different types of threats to computer safety such as viruses, spyware and trojans. Malware is used in malicious attacks like identity theft, phishing and social engineering – threats designed to steal money from unknowing computer users, businesses and banks.

Ransomware is the next level of malware, which restricts access to the computer system that it infects, and sends a message to the user demanding that a ransom be paid in order for the restriction to be removed. Once installed, ransomware will be configured to start automatically when you login to the computer.

One incidence of ransomware infection in 2012 saw victims’ computers display a splash screen displaying the Metropolitan Police Service’s logo. The screen claimed that the victim’s PC was being monitored by the police because they had committed online offences, and demanded a £100 payment.

Phishing

Phishing describes the process of using fake email messages that claim to be from a trusted company or organisation to mislead you into providing private information. These emails appear as expected from these organisations; often with the same brand colours, a visible company logo and a legitimate email message and jargon, making it easy to mistake them for official emails.

How can phishing emails be identified?

- ‘To’ addresses – Be aware of emails with multiple recipients; these can often be fake.
- Subject titles usually have an urgent or exciting claim to get your attention. Look for any spelling mistakes and typos in the subject titles or rest of the email.
- Company logos have no guarantee of legitimacy – don’t trust them.

- Threats – phishing emails will often request information immediately or as a consequence ‘your account will be suspended’.

Social Media

Social networking sites allow the sharing of personal information, opinions and videos or photos. It is important to remember, however, that any information posted on a site could be public and may be seen by lots of people. Most sites allow users to control how public or private information is through privacy settings. It’s important that privacy is controlled to limit the risks of posts being seen by the wrong people.

Don’t provide personal information that e-criminals could use. Don’t list home addresses or telephone numbers. It is a good idea to create a separate e-mail address that is used only with social media sites to protect an identity and to prevent work email addresses being used as a key to accessing company data.

Social media use is on the increase within organisations, yet few companies have policies giving employees guidance about using social media correctly and appropriately.

Without such guidance, organisations run the risk that employees will make mistakes in trying to balance the personal and the professional, which would have a reputational impact and possibly result in legal action for the companies, if used inappropriately.

Be mindful of how employees represent themselves on social networks. Employees must ensure that content associated with them as an identifiable employee of an organisation is consistent with their role and doesn’t compromise the brand’s reputation.

Fraud

First Party Frauds

According to Transactis, a data management company, First Party Fraud is estimated to cost the private sector in the region of £2.6bn a year.

At its most simple, First Party Fraud involves an application for goods or services by a criminal who has no means or intention of paying. However, in recent years the definition has been developed to include other types of fraud.

What to do if you fall victim to first party fraud?

Report it

Fraud committed against Welsh businesses should be reported to Action Fraud, either online;

https://www.actionfraud.police.uk/report or by calling **0300 123 2040**.

Action Fraud is the UK's national fraud reporting centre where you should report fraud if you have been scammed or defrauded.

Synthetic Identity

Synthetic identity fraud is identity theft with a difference; instead of taking an actual person's identity, a fraudster will create a fictional identity by taking pieces of information from a number of people. It may start with an address from one person and then a date of birth from elsewhere.

Victims are often unaware that part of their identity has been stolen in this way and this information is then used to form a credit application, where the aim is to defraud.

Bust Out Fraud

Bust Out Fraud involves a fraudster building up a good credit history and then extending their credit limit or opening a new account before stopping payments completely.

Due to the fraudster utilising a good credit history to apply for further credit, the bank has no grounds on which to turn an application down.

As soon as the credit extension is agreed, the fraudster will then ‘bust out’ and use all the available credit on the account, before letting the account become delinquent.

False Invoicing

In false invoicing schemes, a swindler will send an authentic-looking, professionally-produced invoice for products or services which were never ordered nor received. They do this with the expectation that a percentage of companies won’t pick this up and will process and inevitably pay the invoice without scrutiny.

Unfortunately for many companies, ‘false billers’ are becoming increasingly common, with many cold calling the companies before sending the fake invoice. High pressure from telephone sales people can deceive employees into purchasing a variety of products at unwarranted prices. These sales people may also falsely claim that the business has already ordered the product, either currently or in the past and demand that they receive payment for the order.

These scams can best be avoided by applying reasonable controls in accounts payable procedures and practices within the company, including ensuring that the account staff are aware of all invoices that they are due to receive. Vetting the invoices correctly with unique purchase orders numbers and putting strict payment terms in place will be key to ensuring that the company does not fall foul of ‘false billers’.

What to do if you fall victim to false invoicing?

Report it

Fraud committed against Welsh businesses should be reported to Action Fraud, either online;

https://www.actionfraud.police.uk/report or by calling **0300 123 2040**.

Action Fraud is the UK's national fraud reporting centre where you should report fraud if you have been scammed or defrauded.

Insurance Fraud

Insurance fraud is an illegal act on the part of either the buyer or seller of an insurance contract.

- **Insurance fraud from the issuer** (seller) includes selling policies from non-existent companies, failing to submit premiums and churning policies to create more commissions.
- **Insurance fraud from the buyer** involves attempting to obtain some benefit to which they are not otherwise entitled or when the buyer files a false insurance claim with the intent to defraud an insurance provider out of paying money. The most common type of insurance fraud relates mostly to automobile insurance. The Insurance Fraud Bureau reports that undetected car insurance claims fraud totals £2.1billion per year, adding an additional £50 to the annual costs individual policyholders face, on average, each year
- **"Crash for cash"**: Many scammers are taking to staging collisions, by deliberately putting on their brakes so that the driver behind collides into them. As most insurance providers will state, the fault of the collision is usually attributed to the driver behind and therefore they will pay to fix the damage on both vehicles. This is highly dangerous as fraudsters, motivated by greed, are not only preying on innocent drivers but also putting lives at risk.

- **Ghost accidents**: Sometimes the fraudsters don't crash cars at all and will instead claim back on accidents that didn't even happen. Ghost accidents involve submitting completely fabricated claims for accidents which never actually took place and in some cases for cars that don't even exist.

If you're the insurance provider

Insurance fraud can also be committed when a person provides false information to a company in order to get their insurance cover on more favourable terms, including deliberately underinsuring their vehicle in with the intention of reducing premium costs.

Postal Scams

As more business correspondence has migrated to electronic means, increasingly, e-mails are replacing letters and invoices are being sent via e-mail.

However businesses still rely on the postal service for sending important documents and parcels and some of the most popular scams perpetrated using the postal service are Business Directory Scams. This type of scam will see a business sent a form, generally through the post but occasionally by e-mail or fax, which appears to offer a free listing in a business directory.

The correspondence will request that the recipient returns an order form, even if to refuse the advertising space. According to small print on the form, even by sending the form back the recipient will be committing to an order worth hundreds of pounds a year. If they refuse to pay, legal action will be threatened.

Another popular postal scam involves a card being posted through a door from a parcel delivery service. The card is typical, saying the parcel wasn't delivered and the recipient should call a premium rate number to re-arrange delivery. As soon as the number is called, the caller will be charged a large sum of money for just a few

minutes on the phone.

What to do if you fall victim to a postal scam?

Report it

Fraud committed against Welsh businesses should be reported to Action Fraud, either online;

http://www.actionfraud.police.uk/report or by calling **0300 123 2040**.

Action Fraud is the UK's national fraud reporting centre where you should report fraud if you have been scammed or defrauded.

False Accounting Fraud

False accounting fraud relates to companies overstating their assets or understating their liabilities in order to give the impression that their business is on sounder financial footing that it really is. Whilst false accounting will mainly be motivated by the need to falsify records or alter figures, the reasons for the fraud can vary.

A business's future funding and financing is often dependent on business performance. If banks don't see the business as viable, they won't allow funding. Falsifying accounts will make the business seem more financially viable, making it more appealing to banks. It can also be about the outward image as, by falsifying accounts, businesses can mislead customers into thinking that they are more successful than they actually are.

False accounting fraud can also be perpetrated in other ways. Employees can make inflated expenses claims or falsify accounts to cover up the fact they have stolen money.

Cheque/Cheque Overpayment Fraud

Though cheques aren't used as frequently in personal banking anymore, businesses still rely on them for many transactions, but they can often be counterfeit or forged. Fraudsters can even scam businesses with cheques that have disappearing ink, making it harder to cash cheques for services.

Cheque Overpayment Fraud is an extension of cheque fraud. The fraudster writes a cheque in exchange for goods or services that are in excess of the amount actually owed. Usually, the extra amount will be dressed up as money for something like delivery charges. Fraudsters aim for the business to reimburse the excess amount before realising that the cheque is fraudulent.

This means the effects of fraud are two-fold; the business loses out on the cash for services, while also paying excess cash to the fraudulent party.

What to do if you fall victim to false accounting?

Report it

Fraud committed against Welsh businesses should be reported to Action Fraud, either online;

http://www.actionfraud.police.uk/report or by calling **0300 123 2040**.

Action Fraud is the UK's national fraud reporting centre where you should report fraud if you have been scammed or defrauded.

Mobile Phone Fraud

According to Ofcom, there are currently 82.7million mobile phone subscriptions in the UK with 49% of adults using their mobile phones for internet access. The fact that mobile phones are this ubiquitous means they are easy targets for fraudsters.

Phone calls from companies offering services for PPI claims and personal injury lawyers have become increasingly common and, while many people find them annoying, these type of messages can also be scams. The recipient of a phone call could be asked to call a premium rate phone line and, without realising, could clock up a large phone bill.

These messages are easily dismissed. Recipients can ignore the text or phone call or simply delete it from their phones, but some mobile phone scams aren't as easy to ignore.

Missed call scams are messages from companies purporting to be from PPI companies. This type of fraud will see a criminal register a missed call on someone's phone. Most businesses rely on their mobile phones for remote contact when colleagues are away from their offices and fraudsters hope to take advantage of the owner's curiosity and need to return a missed call for business. Once returned, the call could cost hundreds of pounds.

Fraudsters also hope to take advantage of consumers when they have recently bought a new mobile device. Mobile devices are increasingly costly and complicated and, with so many businesses relying on mobile phones and tablet devices for remote working and working from home, insurance is vital.

Fraudsters will take advantage of this need, calling an individual and offering a deal on mobile insurance that either doesn't exist or isn't fit for purpose. If insurance is bought, a registered provider should always be sought.

Intellectual Property Theft

Intellectual Property (IP) crime is a generic term used to describe a wide range of counterfeiting and piracy offences.

Some of the biggest problem areas – trademark counterfeiting and copyright piracy – are serious IP crimes that defraud consumers, threaten health and safety, impact

significantly on business profits and violate the rights of trademark and copyright owners.

The counterfeiting of imitation products, such as digital media and electrical goods, fashion goods and even food, poses a significant safety threat to consumers worldwide. Unsuspecting customers put their health in jeopardy each time they use counterfeited products such as alcohol and food products, or when they travel in automobiles and aircrafts built with counterfeit parts that are of a substandard quality.

IP crime can also cause considerable financial harm to a business in loss of revenue, as well as reputational damage due to the association with poor-quality goods.

An IP Crime Report details the investigations undergone by Trading Standards Authorities in 2012/13. The report highlights these emerging trends and threats:

- There has been a 27% rise in the amount of investigations into the selling of illicit alcohol
- 64% of responding authorities investigated counterfeit and pirated goods on social media sites, and 69% on websites
- 90% of incidences involving counterfeit goods investigated by Trading Standards involved counterfeit clothing

To protect IP from theft and unauthorised usage, a business must patent its IP assets. Experienced IP lawyers can help discern what can and can't be copyrighted and what IP a business may have.

For advice on reporting Intellectual Property infringements contact the Trading Standards Service: **http://www.tradingstandardswales.org.uk/contact/index.cfm**

The Intellectual Property Office can also offer advice on IP enforcement: **http://www.ipo.gov.uk/ipenforce-ip.htm**

Plastic Card Fraud

Businesses rely on debit cards and credit cards for instant access to their funds. Some businesses have shared access to these cards, meaning credit cards can change hands several times a day, which can cause problems when it comes to security.

These cards can give fraudsters access to vital information about individuals and businesses. No matter how careful its owner is with selecting pins and privacy features, if a card gets stolen or lost it presents a series of worries.

One of the biggest concerns is ‘card not present’ fraud. If the card details fall into the wrong hands, fraudulent transactions can be made over the phone or online without it needing to be present. This can also happen when a card owner may think they are safe. Cards can be skimmed when drawing cash and those details can be used to make transactions.

Skimming

While sometimes it’s easy to see that an ATM machine has been compromised or tampered with, often the devices are well hidden. Sometimes, fraudsters will use a well-concealed camera to record pin details when the user types them in.

Skimming can be hard to detect. There’s no real way to know that an account holder’s details have been compromised until money goes missing or strange transactions start appearing on statements. When that happens, the person’s bank must be informed.

Receipt and Expenses Fraud

In this difficult economic climate, the temptation for theft or fraud has never been higher. Unfortunately for many businesses, an incident of internal fraud can have devastating consequences. What hurts the most: a fraudulent scam from a stranger,

or an internal scam from a company's own employees? An internal fraud scam is not only a risk associated with payroll, but can also have a damaging effect on the company's reputation.

Fraud relating to travel and subsistence is committed when employees who claim back expenses for travel falsely claim more mileage than they used or make claims for journeys that weren't made or for amounts higher than they actually spent.

This type of fraud can also include forged signatures authorising payment, or unauthorised amendments to timesheets. Essentially, the employee is stealing money from the company and possibly from its clients if the claims are charged back to them.

This type of fraud diminishes all trust the employer has in the employee caught committing the scam, as well as having harmful repercussions on their reputation as an employee at future organisations.

Tips to help prevent incidences of employee fraud

- Establish a set of travel and subsistence rules and ensure that they are communicated to employees – ensuring that the consequences of failing to comply with these rules are clear.
- Management should conduct checks of claims against approved work plans, standard mileage for regular destinations and hotel bills and rail tickets.
    - Google Maps can be used to work out a rough idea of accurate mileage
    - Employees can be asked an estimated value before confirming purchase, which can be checked against the claimed value
- Finance teams can be instructed to ensure that correct rates are claimed and that all supporting documents, such as hotel invoices, are included.
- A 'no receipt, no reimbursement' policy can be enforced.
- Ad-hoc checks should be carried out by management to verify details on claims and to ensure that finance teams are being rigorous in their assessments.

If a business has fallen victim to employee fraud contact Action Fraud, either online: **http://www. tradingstandardswales.org.uk/contact/index.cfm** or by calling **0300 123 2040**.

Phishing and Pharming

Businesses can also be ‘phished’ or ‘pharmed’ for their bank details. All e-mail address will have spam e-mails sent to them, and some ‘phishing’ e-mails are designed to look professional, with fraudsters hoping they are convincing enough to draw the vital details out of the person answering the e-mail.

Pharming is similar to phishing. With pharming, fraudsters design fake websites that mimic banks’ official sites in the hope that they are convincing enough for people to enter their online banking information. While the person entering their bank details may think they are accessing a legitimate banking website, their details are being stored by fraudsters to then be used to access their bank accounts.

Application Fraud

Though it’s more commonly grouped with identity fraud, application fraud is an extension of plastic card fraud. With application fraud, a criminal will apply for a credit card or bank account in the name of somebody else. Usually, the fraudster will have prepared for the application by stealing supporting documents from the victim, which are then used to substantiate the fraudster’s claim.

Frequently Used Scamming Tools

Scammers will often have one or more tools that they will use in order to help them commit fraud or theft. These are some of the more frequently used means:

Telephone Numbers

Take note: +4470 numbers are almost exclusively used by scammers.

Personal forwarding phone numbers (also called “UK global redirects”) are easily recognised, and they are a major red flag when it comes to identifying scams or scammers.

The number is often given in the format +447024013818. The +44 country code indicates that the number is UK-based, but don’t be fooled by this little trick.

When given a +4470 number in the course of an email exchange, it is best to assume that the phone number is for a scammer – so it’s best not to call!

Imitation Websites

The most dominant form of communication over the Internet is through websites, but unfortunately detecting their legitimacy can prove a challenge. The website design skills of fraudsters are becoming increasingly sophisticated, and many fraudsters can create and maintain websites with the goal of trying to defraud users. Depending on the skill level of the fraudster, a website can be made to look attractive and legitimate, with the information so appealing that the user can be easily fooled.

These websites are usually hosted outside the UK and are often only ‘live’ for a few days— but that is enough time to trick people into giving up their credit card details or other personal information.

Top Tips for Businesses to Avoid Scams

The rapid growth in technology during the past ten years has meant the ways in which scammers can access money illegitimately has developed at an alarming rate.

Scammers are clever in their approaches and will try any means necessary to succeed in their goal. However, there are a few things that businesses can do to ensure they don’t fall foul of such scams. These are our top tips:

- Always take your time making a business decision over the phone. Legitimate companies won't pressure you to make a snap decision, so don't fall victim to those who ask you for an answer right away.
- Ensure all documents are correctly deleted from the memory when recycling or disposing of old computers and laptops – you will be surprised how easily scammers can still access your personal information by removing the hard drives.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business licence number before progressing with a business transaction. Although scammers may give out false information, ensure you verify the accuracy of these items.
- Don't pay in advance for services. Pay once the service has been delivered and correctly involving before handing over the cash.
- Take caution when dealing business with companies outside the U.K. If a problem occurs with a business transaction, it could be much more difficult to rectify.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Set up Google alerts for "latest scams" and "business crime" to alert yourself to any new scams reported in the news and alert all staff of these.

What to do if you get scammed?

Victims of fraud and scams often wonder where they can turn for help and advice. Police forces across Wales no longer investigate and deal with fraud themselves. Instead, fraud cases are referred to **Action Fraud UK**.

Action Fraud UK is a centralised, specialist fraud reporting centre. Run by the government agency that helps co-ordinate the fight against fraud in the UK, the

National Fraud Authority, it works with the National Fraud Intelligence Bureau to ensure that fraud reports are dealt with by the right people in the right place.

The Action Fraud UK website has a wealth of information relating to all types of fraud and crime, as well as an online fraud reporting service which is accessible at all times of the day. There is also online support available while filling in the form with online advisors available.

Specialist fraud advisers are also available on 0300 123 2040. The lines are open seven days a week.

Action Fraud UK deals with all fraud cases. The only time it is advisable to report fraud to the police is if the crime is underway or if anyone is in immediate danger. The police will take formal reports of fraud in three circumstances:

- If the crime is in progress or about to happen: for example, where a delivery is about to be made or money is at risk
- If the person suspected of committing fraud is known locally and can be easily identified
- If the victim of the crime is vulnerable. They may not necessarily have access or be able to use the telephone to report or be able to report it via the internet so they will require support from the police to assist in reporting the crime

If bank cards or bank details have been used by fraudsters, the bank must be informed before they can make a report to the National Fraud Intelligence Bureau. In these circumstances, the victim may not be required to do anything unless:

- The card/account involved is not a UK bank or financial institution
- The bank will not reimburse the victim or they have specifically requested the victim makes a report
- The victim holds information that may identify the perpetrator

Reporting Online Scams

Many websites have their own tools for reporting fraudulent adverts or e-mails; for example Twitter allows users to report and block users they believe to be spammers.

Phishing e-mails can be reported through the Action Fraud website.

Top Ten Checklist

1. Always read the small print and Terms & Conditions

   companies might hide away clauses in the T&Cs that people don't even read. These clauses could cost you a lot of money.

2. If you think it's too good to be true, it probably is

   If you are offered a great deal, designer clothing for cheap or some computer software on the cheap, be suspicious. The deal is probably too good to be true. Counterfeit goods might be a great deal, but the quality won't be as good.

3. Don't reply to e-mails asking for personal data

   Unsolicited e-mails asking for personal data and information should never be replied to. Only give personal information over secure connections, to reputable sites.

4. Be smart with your passwords

   Change them regularly and don't make them too obvious. Recent data showed that 123456 are the most commonly used passwords.

5. Draw up a social media policy

   With more and more people being arrested for offensive comments on Twitter,

ensuring best practice amongst employees is vital. A social media policy will give these people guidance.

6. Encrypt data

   Encrypting data won't stop it from being stolen but it will mean that the hacker won't be able to access it.

7. Physical security

   Ensuring that a business's physical security is comprehensive will ensure that people in the building are accounted for. If important documents and information have restricted access from within the building, then that also curtails threats.

8. Ensure your books are up-to-date

   When tracking invoices, payments and others, it's vital that tracking ledgers and books are regularly updated. This means that if a rogue invoice comes through, you would be more likely to be able to pinpoint it.

9. Report suspicious activity

   If you've received a suspicious letter, e-mail or phone call, report it to the relevant authorities.

10. Be vigilant

    A lot of people fall foul to scams and fraud due to not being vigilant enough. If you are suspicious about a cash machine or an invoice, don't use it or pay it until you have investigated.

For more information refer to our **accessibility statement**.